<RH>

REVA UNIVERSITY
Bengaluru, India

REVA HACK 2023

TECHNOLOGY BEYOND IMAGINATION

Powered by: IEEE

PROJECT TITLE : Hardware Based Password Manager

TEAM NAME: idkWhatWe’reDoing

TEAM LEAD: M Aswartha Reddy m.aswarthreddy@gmail.com

TEAM MEMBERS:

D K Bharath Reddy	cricketers213@gmail.com
Pulkit Dhamija	pulkit.dhamijas@gmail.com
Nidhi Prakash	nidhip03@gmail.com
Shishria M Iyar	shishiraiyar@gmail.com

PROBLEM STATEMENT :

- Password security is of paramount importance in today's digital landscape, where individuals and organizations rely heavily on online services, websites, and various digital platforms.
- Passwords serve as the primary defense mechanism for protecting personal and sensitive information, and their strength and integrity are crucial in preventing unauthorized access and potential data breaches.
- Software-based password manager offers convenience and security by enabling users to store and manage their passwords digitally. However, it also comes with its own set of challenges and risks such as Single Point of Failure: With software-based password managers, users typically need to remember one master password to access their entire password database. If this master password is compromised or forgotten, it can lead to a complete loss of access to all stored passwords.
- In case the cloud service is compromised, all the passwords are exposed to the public.
- Thus it is imperative that we switch to hardware based password management system to enhance the security and ensure privacy of the user.

Tracks available

1. GEN AI
2. BLOCKCHAIN
3. AR VR
4. CLOUD AND IOT
5. CYBER SECURITY

CHOICE OF TRACK: Cyber Security

OPPORTUNITY – How different is it from existing ideas out there

Drawbacks of using Software Password Manager

- The main objective is to avoid any communication with the internet, which is a huge bottleneck for security in software-based password managers such as Google password manager, LastPass, KeePass. Most of the widely available password managers, merely encrypt the password and store them on the cloud, making them vulnerable to database breaches.
- Another major issue for password leaks is phishing, in which users are tricked into revealing sensitive information, which may include passwords. Also, most of them repeat passwords for multiple accounts as it is a hassle to remember many strong passwords.
- We plan on eliminating the issue of cloud database breaches by storing the encrypted passwords locally, on chip. There may be cases where the user would like to have backups of their passwords, in case they lose the device. Hence a facility will be provided to backup the passwords on to an auxiliary flash storage, which the user can store in a secure place. Since there is no way to decrypt the passwords without the master passwords, there is no worry even if the contents of the flash are read by an unwanted person.

OPPORTUNITY – How different is it from existing ideas out there

Comparison between hardware and software password managers

Comparison Factors	Software-Based Password Management System	Hardware-Based Password Management System
Vulnerability	Susceptible to malware, keyloggers, phishing attacks	Immune to common malware threats
Single Point of Failure	Master password vulnerability can compromise all stored passwords	Even with physical possession and user verification the stored passwords cannot be compromised because of zero knowledge proof
Portability	Dependent on devices and synchronization capabilities	Portable, not dependent on specific devices or internet connectivity
Protection Against Malware	Prone to malware attacks on the host device	Not affected by keyloggers or screen capture attacks

OPPORTUNITY – How will it be able to solve the problem

- The Hardware Password Manager is based on the concept of zero knowledge proof, to store encrypted passwords in a secure manner.
- Users can store their passwords on the device, which is unlocked with the help of a master password. The approach behind this project will be to encrypt users' passwords in a secure manner using AES-256.
- The crucial building block of this project is that the key for decrypting user passwords is not stored on the device. The key for these user passwords is a SHA-256 hash of the master password.
- This hash is used as the key for the AES algorithm to encrypt user passwords and only the encrypted password is stored on the device flash.
- When the user wants to retrieve any password, the master password must be entered, which is use to compute the hash which is then validated, to check if the entered password is correct.
- Once the validation is completed, the user can select the required account for which the password is required.

SOLUTION

- The hardware-based password manager uses a microcontroller ESP32 that securely stores a user's passwords.
- When connected to a computer, it allows the user to select the desired account. With a simple click on a rotary encoder, the microcontroller reads the encrypted password from the flash and is decrypted using the hash of the master password. This password is sent as a series of keystrokes to the host computer using HID emulation, thus automatically entering password, eliminating the need for manual entry.
- This streamlined process ensures efficient and convenient access to various accounts while maintaining a high level of security. The device serves as a reliable and user-friendly solution for managing multiple passwords in a hardware-encrypted environment.

TECHNOLOGY USED

Hardware

- **ESP32** to carry out encryption and decryption operations
- **Rotary Encoder** for taking in user input
- **DS1307 RTC** to store encrypted data and maintain time
- **OLED Display**
- **Buzzer**

Software

- **Arduino IDE**
- **SHA-256** to hash master password
- **AES-256** to encrypt user accounts and password
- **Flask-Python** to provide user interface for taking backups

WHY SHOULD WE CHOOSE YOUR TEAM?

Expertise in hardware and software integration helps us in building a unique solution

In this age of cyber attacks, we would like to provide a reliable solution which is easy to use, even by non tech savvy users

Diverse skillset of our team members ensure we can collaborate and come with a solution at the end of the hackathon

Won 6+ hackathons and participated in various other hackathons, placing in the top 3